REMARKS

The undersigned and the inventor, Norman Margolus, had a personal interview on April 21, 2004 with the examiner, Hung Q. Pham, and his supervisor, Shahid Alam. The discussion at the interview included a presentation of the above amendments to claim 1 (and amendments to claim 68, which is being pursued in a continuation application) and a discussion of the differences between claims 1 and 68 and the examiner's prior art references in his final action of January 9, 2004 (Wong, Brady, Whiting). The examiner's suggested change to the claim ("having a second client program initiate a process for depositing") has been made. A minor improvement in claim language has also been made since the interview; in the interview claim, items were referred to as being deposited "in a network", whereas the claim presented herein refers to depositing "in a data repository". A new dependent claim (175) has been added to give an example of how physical locations can differ.

The examiner indicated (see Examiner's Interview Summary) that: "The proposed amendment was discussed, and the proposed changes overcome the Final Action. However, the restriction may be applied based on these two claims." In light of the examiner's concerns as to a restriction, it was agreed that claim 68 and its related dependent claims would be pursued in a continuation application, which is being filed on the same date as this amendment.

The examiner had rejected claim 1 under 35 USC 103(a) as being unpatentable over Wong (US 6557102) in view of Brady (US 5914938). The examiner agreed at the interview that the amendments made to claim 1 have overcome that rejection.

As noted at the interview, amended claim 1 differs from the prior art in at least three very significant ways.[1]

First, claim 1 requires that the digital fingerprint be used to store the data item at a physical location or locations associated with the digital fingerprint so that pseudorandomness is introduced into the physical location. The relevant claim language is:

[1] We do not mean to suggest that there are not other ways in which the claim differs from the prior art.

determining a digital fingerprint from the data item using a reproducible pseudorandom process that produces digital fingerprints having a pseudorandom distribution; and

storing the data item in the data repository at a physical location or locations associated with the digital fingerprint,

* * *

wherein the pseudorandom distribution of the digital fingerprints introduces pseudorandomness into the physical location at which data items are stored in the data repository.

Second, claim 1 requires a type of digital fingerprint that to a high degree of probability is unique for every distinct data item. The claim language is as follows:

wherein the reproducible pseudorandom process produces a digital fingerprint adapted to probabilistically guarantee to provide a unique digital fingerprint for every distinct data item sent to the data repository.

Third, claim 1 requires that, upon a second attempt being made to deposit a data item, the digital fingerprint be used to determine whether the data item is already stored in the network. The language is as follows:

having a second client program initiate a process for depositing a second data item in the data repository, wherein the second data item is identical to the data item stored by the first client program, the depositing including

determining a digital fingerprint from the second data item using the reproducible pseudorandom process; and

determining from the digital fingerprint that a data item identical to the second data item is already stored in the data repository; and

relying on the data item already stored in the data repository for storage of the second data item rather than storing a separate copy of the second data item.

Neither Wong nor Brady, either alone or in combination, teach the above referenced limitations of claim 1.

Wong teaches that digital fingerprints be used for authentication (specifically, of medical images). There is no suggestion of any use of digital fingerprints for storage purposes, and thus, of course, there is no suggestion of using digital fingerprints for storing a data item at a location associated with the digital fingerprint, or of using a digital fingerprint to determine whether an item is already stored.

Brady teaches that digital fingerprints (hashes) be used for compressing a long database key to a smaller hashed key for saving storage space. The hashed key points to the location of the original key. The type of process used to produce the digital fingerprint anticipates that the fingerprint is not unique for every distinct key. It is expected that collisions will occur (different keys producing the same fingerprint), and provisions are taken to deal with the collisions. There is also no use made of the digital fingerprint to determine whether a data item is already in storage.

The remaining claims are all properly dependent on claim 1, and thus allowable therewith. Each of the dependent claims adds one or more further limitations that enhance patentability, but those limitations are not presently relied upon. For that reason, and not because applicants agree with the examiner, no rebuttal is offered to the examiner's reasons for rejecting the dependent claims.

Allowance of the application is requested.

Please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 6/17/04

G. Roger Lee
Reg. No. 28,963

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110-2804
Telephone: (617) 542-5070
Facsimile: (617) 542-8906

20870046.doc